

# Mixed orthogonal arrays, $(u, m, \mathbf{e}, s)$ -nets, and $(u, \mathbf{e}, s)$ -sequences

Peter Kritzer\* and Harald Niederreiter

July 1, 2015

## Abstract

We study the classes of  $(u, m, \mathbf{e}, s)$ -nets and  $(u, \mathbf{e}, s)$ -sequences, which are generalizations of  $(u, m, s)$ -nets and  $(u, s)$ -sequences, respectively. We show equivalence results that link the existence of  $(u, m, \mathbf{e}, s)$ -nets and so-called mixed (ordered) orthogonal arrays, thereby generalizing earlier results by Lawrence, and Mullen and Schmid. We use this combinatorial equivalence principle to obtain new results on the possible parameter configurations of  $(u, m, \mathbf{e}, s)$ -nets and  $(u, \mathbf{e}, s)$ -sequences, which generalize in particular a result of Martin and Stinson.

**Keywords:**  $(u, m, \mathbf{e}, s)$ -net,  $(u, \mathbf{e}, s)$ -sequence, orthogonal array, ordered orthogonal array, mixed orthogonal array.

**2010 MSC:** 05B15, 11K06, 11K38.

## 1 Introduction and basic definitions

The construction of point sets and sequences with good equidistribution properties is a classical problem in number theory and has important applications to quasi-Monte Carlo methods in numerical analysis (see the books of Dick and Pillichshammer [1], Leobacher and Pillichshammer [8], and Niederreiter [13]). The standard setting is that of the  $s$ -dimensional unit cube  $[0, 1]^s$ , for a given dimension  $s \geq 1$ , from which the points are taken. While the problem of constructing evenly distributed points in  $[0, 1]^s$  is of number-theoretic origin, it also has a strong combinatorial flavor (see [1, Chapter 6] and [7, Chapter 15]).

Powerful methods for the construction of finite point sets with good equidistribution properties in  $[0, 1]^s$  are based on the theory of nets (see again the references above as well as the original paper [12] and the recent handbook article [14]). This theory was recently extended by Tezuka [20] and studied in a slightly modified form by Hofer [3], Hofer and Niederreiter [4], Kritzer and Niederreiter [5], and Niederreiter and Yeo [17]. The underlying idea of these nets is to guarantee perfect equidistribution of the points for certain subintervals of the half-open unit cube  $[0, 1)^s$ . Concretely, for a dimension  $s \geq 1$

---

\*P. Kritzer is supported by the Austrian Science Fund (FWF) Project F5506-N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

and an integer  $b \geq 2$ , an interval  $J \subseteq [0, 1]^s$  is called an *elementary interval in base  $b$*  if it is of the form

$$J = \prod_{i=1}^s [a_i b^{-d_i}, (a_i + 1) b^{-d_i}) \quad (1)$$

with integers  $d_i \geq 0$  and  $0 \leq a_i < b^{d_i}$  for  $1 \leq i \leq s$ . These intervals play a crucial role in the subsequent definition of a  $(u, m, \mathbf{e}, s)$ -net, which we state below. Here and in the following, we denote by  $\mathbb{N}$  the set of positive integers and by  $\lambda_s$  the  $s$ -dimensional Lebesgue measure.

**Definition 1.** Let  $b \geq 2$ ,  $s \geq 1$ , and  $0 \leq u \leq m$  be integers and let  $\mathbf{e} = (e_1, \dots, e_s) \in \mathbb{N}^s$ . A point set  $\mathcal{P}$  of  $b^m$  points in  $[0, 1]^s$  is a  $(u, m, \mathbf{e}, s)$ -net in base  $b$  if every elementary interval  $J \subseteq [0, 1]^s$  in base  $b$  of volume  $\lambda_s(J) \geq b^{u-m}$  and of the form (1), with integers  $d_i \geq 0$ ,  $0 \leq a_i < b^{d_i}$ , and  $e_i | d_i$  for  $1 \leq i \leq s$ , contains exactly  $b^m \lambda_s(J)$  points of  $\mathcal{P}$ .

Definition 1 is the definition of a  $(u, m, \mathbf{e}, s)$ -net in base  $b$  in the sense of [4]. Previously, Tezuka [20] introduced a slightly more general definition where the conditions on the number of points in the elementary intervals need to hold only for those elementary intervals  $J$  in base  $b$  with  $\lambda_s(J) = b^{u-m}$ . The narrower definition in [4] guarantees, as stated in that paper, that every  $(u, m, \mathbf{e}, s)$ -net in base  $b$  is also a  $(v, m, \mathbf{e}, s)$ -net in base  $b$  for every integer  $v$  with  $u \leq v \leq m$ . The latter property is very useful when working with such point sets (see again [4] for further details). Hence, whenever we speak of a  $(u, m, \mathbf{e}, s)$ -net here, we mean a  $(u, m, \mathbf{e}, s)$ -net in the narrower sense of Definition 1.

Note that the points of a  $(u, m, \mathbf{e}, s)$ -net tend to be very evenly distributed if  $u$  is small. But the choice of  $e_1, \dots, e_s \in \mathbb{N}$  also plays an important role since larger values of the  $e_i$  in general entail fewer restrictions in the defining property of the net.

For infinite sequences of points in  $[0, 1]^s$  with good equidistribution properties, the corresponding concept is that of a  $(u, \mathbf{e}, s)$ -sequence. As usual, we write  $[\mathbf{x}]_{b,m}$  for the coordinatewise  $m$ -digit truncation in base  $b$  of  $\mathbf{x} \in [0, 1]^s$  (compare with [14, Remark 14.8.45] and [15, p. 194]).

**Definition 2.** Let  $b \geq 2$ ,  $s \geq 1$ , and  $u \geq 0$  be integers and let  $\mathbf{e} \in \mathbb{N}^s$ . A sequence  $\mathbf{x}_1, \mathbf{x}_2, \dots$  of points in  $[0, 1]^s$  is a  $(u, \mathbf{e}, s)$ -sequence in base  $b$  if for all integers  $g \geq 0$  and  $m > u$ , the points  $[\mathbf{x}_n]_{b,m}$  with  $gb^m < n \leq (g+1)b^m$  form a  $(u, m, \mathbf{e}, s)$ -net in base  $b$ .

Again, the points of a  $(u, \mathbf{e}, s)$ -sequence are very evenly distributed if  $u$  is small, but also in this case the choice of  $\mathbf{e}$  has an influence on the manner in which the points are spread over the elementary intervals in the unit cube.

If we choose  $\mathbf{e} = (1, \dots, 1) \in \mathbb{N}^s$  in Definitions 1 and 2, then these definitions coincide with those of a classical  $(u, m, s)$ -net and a classical  $(u, s)$ -sequence, respectively. The reasons why the more general  $(u, m, \mathbf{e}, s)$ -nets and  $(u, \mathbf{e}, s)$ -sequences were introduced have to do with their applications to quasi-Monte Carlo methods. Since this paper is devoted to the combinatorial aspects of  $(u, m, \mathbf{e}, s)$ -nets and  $(u, \mathbf{e}, s)$ -sequences, we do not elaborate on these reasons and we refer instead to [5, Section 1] and [20].

It was shown by Lawrence [6] and Mullen and Schmid [11] that classical  $(u, m, s)$ -nets are combinatorially equivalent to certain types of orthogonal arrays (see also [1, Section 6.2] for an exposition of this result). This equivalence has important implications for the theory of  $(u, m, s)$ -nets and  $(u, s)$ -sequences (see [1, Chapter 6] and [18]). The main result of the present paper generalizes this equivalence to  $(u, m, \mathbf{e}, s)$ -nets (see Theorem 5).

The crucial step is to move from orthogonal arrays to mixed orthogonal arrays in the sense of [2, Chapter 9]. We recall the definition of a mixed orthogonal array  $\text{OA}(N, l_1^{k_1} \cdots l_v^{k_v}, t)$  from [2, Definition 9.1], where we change the notation from  $s_i$  to  $l_i$  since in our case  $s$  stands for a dimension. We write  $R(b) = \{0, 1, \dots, b-1\} \subset \mathbb{Z}$  for every integer  $b \geq 2$ .

**Definition 3.** Let  $N \geq 1$ ,  $l_1, \dots, l_v \geq 2$ ,  $k_1, \dots, k_v \geq 1$ , and  $0 \leq t \leq k := k_1 + \cdots + k_v$  be integers. A *mixed orthogonal array*  $\text{OA}(N, l_1^{k_1} \cdots l_v^{k_v}, t)$  is an array of size  $N \times k$  in which the first  $k_1$  columns have symbols from  $R(l_1)$ , the next  $k_2$  columns have symbols from  $R(l_2)$ , and so on, with the property that in any  $N \times t$  subarray every possible  $t$ -tuple occurs an equal number of times as a row.

**Remark 1.** The parameter  $t$  of a mixed orthogonal array is called its *strength*. Definition 3 is vacuously satisfied for  $t = 0$ . As in [2, Definition 9.1], it is not required that  $l_1, \dots, l_v$  be distinct. If  $l_1 = \cdots = l_v$ , then Definition 3 reduces to that of an orthogonal array (see [2, Definition 1.1]).

Further results of this paper concern bounds on the parameters of  $(u, m, \mathbf{e}, s)$ -nets and  $(u, \mathbf{e}, s)$ -sequences for the case of greatest practical interest where  $u = 0$  (see Theorems 1 to 4). Moreover, we show a necessary condition for the parameters of a mixed ordered orthogonal array (see Theorem 6) which generalizes [10, Lemma 3.1].

## 2 Necessary conditions for $(0, m, \mathbf{e}, s)$ -nets

The parameter  $u$  of a  $(u, m, \mathbf{e}, s)$ -net is a nonnegative integer and its optimal value is  $u = 0$ . The following result imposes a combinatorial obstruction on the existence of  $(0, m, \mathbf{e}, s)$ -nets. If  $\mathbf{e} = (e_1, \dots, e_s) \in \mathbb{N}^s$ , then we can assume without loss of generality that  $e_1 \leq e_2 \leq \cdots \leq e_s$ .

**Theorem 1.** Let  $\mathbf{e} = (e_1, \dots, e_s) \in \mathbb{N}^s$  with  $e_1 \leq e_2 \leq \cdots \leq e_s$ . For  $2 \leq t \leq s$  and  $m \geq e_{s-t+1} + \cdots + e_{s-1} + e_s$ , the existence of a  $(0, m, \mathbf{e}, s)$ -net in base  $b$  implies the existence of a mixed orthogonal array  $\text{OA}(b^m, l_1^1 \cdots l_s^1, t)$  with  $l_i = b^{e_i}$  for  $1 \leq i \leq s$ .

*Proof.* Let  $\mathcal{P}$  be a  $(0, m, \mathbf{e}, s)$ -net in base  $b$  and let the points of  $\mathcal{P}$  be

$$\mathbf{x}_n = (x_n^{(1)}, \dots, x_n^{(s)}) \in [0, 1]^s \quad \text{for } n = 1, \dots, b^m.$$

Furthermore, define

$$z_i(n) = \lfloor b^{e_i} x_n^{(i)} \rfloor \in R(b^{e_i}) \quad \text{for } 1 \leq n \leq b^m, 1 \leq i \leq s.$$

Arrange these integers into the  $b^m \times s$  array

$$(z_i(n))_{1 \leq n \leq b^m, 1 \leq i \leq s} = \begin{pmatrix} z_1(1) & z_2(1) & \cdots & z_s(1) \\ z_1(2) & z_2(2) & \cdots & z_s(2) \\ \vdots & \vdots & & \vdots \\ z_1(b^m) & z_2(b^m) & \cdots & z_s(b^m) \end{pmatrix}. \quad (2)$$

For  $i = 1, \dots, s$ , let  $\mathbf{z}_i$  denote the  $i$ th column of the array in (2). Choose a strength  $t$  with  $2 \leq t \leq s$  and assume that  $m \geq e_{s-t+1} + \cdots + e_{s-1} + e_s$ , i.e., that  $m$  is at least

as large as the sum of the  $t$  largest  $e_i$ . Pick  $1 \leq i_1 < i_2 < \dots < i_t \leq s$  and consider the corresponding columns  $\mathbf{z}_{i_1}, \dots, \mathbf{z}_{i_t}$ . We have to show that  $\mathbf{z}_{i_1}, \dots, \mathbf{z}_{i_t}$  are orthogonal in the sense of Definition 3, namely that every possible  $t$ -tuple occurs an equal number of times as a row in the  $b^m \times t$  subarray formed by the columns  $\mathbf{z}_{i_1}, \dots, \mathbf{z}_{i_t}$ . Take any  $h_j \in R(b^{e_{i_j}})$  for  $1 \leq j \leq t$ . For  $1 \leq n \leq b^m$  we have  $(z_{i_1}(n), \dots, z_{i_t}(n)) = (h_1, \dots, h_t)$  if and only if  $z_{i_j}(n) = h_j$  for  $1 \leq j \leq t$ , which is equivalent to  $\left\lfloor b^{e_{i_j}} x_n^{(i_j)} \right\rfloor = h_j$  for  $1 \leq j \leq t$ . The latter condition holds if and only if

$$\mathbf{x}_n \in J := \prod_{i=1}^s J_i,$$

where

$$J_i = \begin{cases} [h_j b^{-e_{i_j}}, (h_j + 1) b^{-e_{i_j}}) & \text{if } i = i_j \text{ for some } j \in \{1, \dots, t\}, \\ [0, 1) & \text{otherwise.} \end{cases}$$

Now  $\lambda_s(J) = b^{-e_{i_1} - \dots - e_{i_t}} \geq b^{-e_{s-t+1} - \dots - e_s} \geq b^{-m}$ , and so  $J$  is an elementary interval in base  $b$  to which the definition of a  $(0, m, \mathbf{e}, s)$ -net in base  $b$  applies. Therefore the number of integers  $n$  with  $1 \leq n \leq b^m$  such that  $(z_{i_1}(n), \dots, z_{i_t}(n)) = (h_1, \dots, h_t)$  is given by

$$A(J, \mathcal{P}) = b^m \lambda_s(J) = b^m b^{-e_{i_1} - \dots - e_{i_t}}$$

for all  $(h_1, \dots, h_t)$ , and the desired orthogonality property is established.  $\square$

**Remark 2.** We can also combine  $e_i$  that are equal, say we have  $k_1$  of the  $e_i$  equal to 1,  $k_2$  of the  $e_i$  equal to 2, and so on up to  $k_v$  of the  $e_i$  equal to  $v$  with  $\sum_{h=1}^v k_h = s$ . Then we obtain a mixed orthogonal array  $\text{OA}(b^m, b^{k_1}(b^2)^{k_2} \dots (b^v)^{k_v}, t)$ , where in  $b^{k_1}(b^2)^{k_2} \dots (b^v)^{k_v}$  we delete the parts  $(b^h)^{k_h}$  with  $k_h = 0$ .

In view of Theorem 1, we can apply the Rao bound for mixed orthogonal arrays. This bound is given in [2, Theorem 9.4] and reads as follows in our notation (we again change the  $s_i$  to  $l_i$  in comparison to [2]). The cases of even and odd strength  $t$  have to be distinguished. For binomial coefficients, we use the standard convention  $\binom{k}{r} = 0$  for  $r > k$ .

**Proposition 1.** *The parameters of an  $\text{OA}(N, l_1^{k_1} \dots l_v^{k_v}, t)$ , where without loss of generality  $l_1 \leq l_2 \leq \dots \leq l_v$ , satisfy*

$$N \geq \sum_{j=0}^g \sum_{I_j(v)} \binom{k_1}{r_1} \dots \binom{k_v}{r_v} (l_1 - 1)^{r_1} \dots (l_v - 1)^{r_v} \quad (3)$$

if  $t = 2g$ , and

$$\begin{aligned} N &\geq \sum_{j=0}^g \sum_{I_j(v)} \binom{k_1}{r_1} \dots \binom{k_v}{r_v} (l_1 - 1)^{r_1} \dots (l_v - 1)^{r_v} \\ &\quad + \sum_{I_g(v)} \binom{k_1}{r_1} \dots \binom{k_{v-1}}{r_{v-1}} \binom{k_v - 1}{r_v} (l_1 - 1)^{r_1} \dots (l_{v-1} - 1)^{r_{v-1}} (l_v - 1)^{r_v + 1} \end{aligned} \quad (4)$$

if  $t = 2g + 1$ , where

$$I_j(v) := \left\{ (r_1, \dots, r_v) \in \mathbb{N}_0^v : \sum_{i=1}^v r_i = j \right\},$$

$\sum_{I_j(v)}$  denotes a sum over all  $v$ -tuples  $(r_1, \dots, r_v)$  in  $I_j(v)$ , and  $\mathbb{N}_0$  is the set of nonnegative integers.

We can apply the Rao bound to the mixed orthogonal arrays obtained from  $(0, m, \mathbf{e}, s)$ -nets. Let us start with the case where the strength  $t$  is even. We recall our assumption  $e_1 \leq e_2 \leq \dots \leq e_s$ .

**Theorem 2.** *Let  $b \geq 2$  and  $s \geq 2$  be integers and let  $g$  be an integer with  $1 \leq g \leq s/2$ . If there exists a  $(0, m, \mathbf{e}, s)$ -net in base  $b$  with  $m \geq e_{s-2g+1} + \dots + e_{s-1} + e_s$ , then necessarily*

$$\sum_{j=1}^g \sum_{1 \leq i_1 < \dots < i_j \leq s} (b^{e_{i_1}} - 1) \dots (b^{e_{i_j}} - 1) \leq b^m - 1.$$

*Proof.* We apply the Rao bound in Proposition 1 with  $N = b^m$ , strength  $t = 2g$ ,  $v = s$ ,  $k_i = 1$  for  $1 \leq i \leq s$ , and  $l_i = b^{e_i}$  for  $1 \leq i \leq s$ . Then from (3) we get

$$b^m \geq \sum_{j=0}^g \sum_{I_j(s)} \binom{1}{r_1} \dots \binom{1}{r_s} (l_1 - 1)^{r_1} \dots (l_s - 1)^{r_s}.$$

The contribution to the outer sum over  $j$  for  $j = 0$  is equal to 1. For  $1 \leq j \leq g$ , we use that  $\binom{1}{r} = 1$  for  $r = 0, 1$  and  $\binom{1}{r} = 0$  for  $r \geq 2$ . Hence it suffices to restrict the sum over  $I_j(s)$  to the subset

$$\left\{ (r_1, \dots, r_s) \in \{0, 1\}^s : \sum_{i=1}^s r_i = j \right\}.$$

This yields the desired bound.  $\square$

For odd  $t$ , the Rao bound for mixed orthogonal arrays obtained from  $(0, m, \mathbf{e}, s)$ -nets attains the following form (the proof of Theorem 3 is similar to that of Theorem 2).

**Theorem 3.** *Let  $b \geq 2$  and  $s \geq 3$  be integers and let  $g$  be an integer with  $1 \leq g \leq (s-1)/2$ . If there exists a  $(0, m, \mathbf{e}, s)$ -net in base  $b$  with  $m \geq e_{s-2g} + \dots + e_{s-1} + e_s$ , then necessarily*

$$\sum_{j=1}^g \sum_{1 \leq i_1 < \dots < i_j \leq s} (b^{e_{i_1}} - 1) \dots (b^{e_{i_j}} - 1) + (b^{e_s} - 1) \sum_{1 \leq i_1 < \dots < i_g \leq s-1} (b^{e_{i_1}} - 1) \dots (b^{e_{i_g}} - 1) \leq b^m - 1.$$

**Remark 3.** It is a natural question whether the Rao bound yields different results depending on whether one lumps together identical  $e_i$  or not. The answer to this question is negative. We consider the Rao bound in two different versions, where we distinguish the parameters by marking them with superscripts (NL) for the case where there is “no lumping” and (L) where there is “lumping”. To be more precise, there are two different situations: (i) the case where we do not lump together the  $e_i$  with the same value—in this case, we count  $v^{(\text{NL})} = s$  values of the  $l_i^{(\text{NL})}$ , and  $k_1^{(\text{NL})} = \dots = k_s^{(\text{NL})} = 1$ ; (ii) the case where we do lump together the  $e_i$  with the same value—in this case, we count

$v = v^{(L)} \leq s$  different values of the  $l_i^{(L)}$  and  $k_1^{(L)}, \dots, k_v^{(L)} \geq 1$  with  $\sum_{h=1}^v k_h^{(L)} = s$ . We consider for simplicity the case where  $t$  is even and we claim that for every  $u \in \mathbb{N}$ , the right-hand side of the Rao bound (3) has the same value for the cases (i) and (ii). For the proof, we take real numbers  $y_1, \dots, y_s$ , a variable  $X$ , and the polynomial given by the product  $\prod_{i=1}^s (1 + y_i X)$ . We write this polynomial in the form

$$\prod_{i=1}^s \left( \sum_{r=0}^{\infty} \binom{1}{r} y_i^r X^r \right) = \prod_{h=1}^v (1 + b_h X)^{k_h} = \prod_{h=1}^v \left( \sum_{r=0}^{\infty} \binom{k_h}{r} b_h^r X^r \right). \quad (5)$$

Here  $k_h$  of the  $y_i$  are equal to  $b_h$  for  $1 \leq h \leq v$  and  $\sum_{h=1}^v k_h = s$ . For  $j = 0, 1, \dots, g$ , we compare the coefficients of  $X^j$  on the leftmost and rightmost side of (5), then we sum over  $j = 0, 1, \dots, u$ , and finally we substitute  $y_i = l_i^{(NL)}$  for  $1 \leq i \leq s$ , thus proving the claim.

### 3 Necessary conditions for $(0, \mathbf{e}, s)$ -sequences

In this section, we derive some necessary conditions for the existence of  $(0, \mathbf{e}, s)$ -sequences. First of all, we note that, by using [5, Proposition 4], we obtain necessary conditions on the parameters of  $(0, \mathbf{e}, s)$ -sequences in base  $b$  from the necessary conditions on the parameters of  $(0, m, \mathbf{e}, s)$ -nets in base  $b$  stated in Section 2. However, there are further conditions that we can derive, as we will now show.

If not stated otherwise, we assume throughout this section that, without loss of generality, the entries  $e_i$  of the  $s$ -tuple  $\mathbf{e} \in \mathbb{N}^s$  are ordered in a nondecreasing manner, i.e., the first  $k_1$  entries of  $\mathbf{e}$  are equal to 1, the next  $k_2$  entries of  $\mathbf{e}$  are equal to 2, etc., where the  $k_r$  are nonnegative integers.

**Theorem 4.** *For every  $(0, \mathbf{e}, s)$ -sequence in base  $b$  for which  $k_r$  of the  $e_i$  are equal to  $r$  for all  $r \in \mathbb{N}$  and some nonnegative integers  $k_r$ , we must have  $k_r \leq b^r$  for all  $r \in \mathbb{N}$ .*

*Proof.* For a  $k_r > 0$ , we consider the projection of the given sequence onto those coordinates that correspond to the  $e_i$  with  $e_i = r$ . This projection yields a  $(0, \mathbf{r}, k_r)$ -sequence in base  $b$  with  $\mathbf{r} = (r, \dots, r) \in \mathbb{N}^{k_r}$ . By using [5, Theorem 4], we obtain a  $(0, k_r)$ -sequence in base  $b^r$ . However, it is well known from the theory of classical  $(u, s)$ -sequences that a  $(0, k_r)$ -sequence in base  $b^r$  can exist only if  $k_r \leq b^r$  (see [1, Corollary 4.36] and [13, Corollary 4.24]). The same principle can be applied to all  $k_r > 0$ .  $\square$

**Remark 4.** The bound  $k_r \leq b^r$  in Theorem 4 is essentially best possible for prime powers  $b$ . Indeed, suppose that  $b = q$  is a prime power. We consider a Niederreiter sequence in base  $q$  for which we use all monic irreducible polynomials over the finite field  $\mathbb{F}_q$  (ordered according to their degrees in a nondecreasing manner) as the generating polynomials (see [1, Section 8.1] for the theory of Niederreiter sequences). Then by a result of Tezuka [20], for every  $s \in \mathbb{N}$  the  $s$ -dimensional version of this sequence is a  $(0, \mathbf{e}, s)$ -sequence in base  $q$ , where  $\mathbf{e} = (e_1, \dots, e_s)$  with  $e_i$  being the degree of the  $i$ th generating polynomial for  $1 \leq i \leq s$ . On the other hand, in this case we have for every  $r \in \mathbb{N}$  that  $k_r = N_q(r)$ , where  $N_q(r)$  denotes the number of monic irreducible polynomials over  $\mathbb{F}_q$  of degree  $r$ . It is well known that  $N_q(r)$  has the order of magnitude  $q^r/r$  (see [9, Theorem 3.25]), which differs only by the factor  $r$  from the upper bound  $q^r$  on  $k_r$ .

We can extend the principle in Theorem 4 further. Suppose that we are given a  $(0, \mathbf{e}, s)$ -sequence in base  $b$  for which  $k_r \in \mathbb{N}_0$  of the  $e_i$  are equal to  $r$  for  $r \in \mathbb{N}$ . Now we consider a collection of positive  $k_{r_1}, k_{r_2}, \dots, k_{r_w}$ , where the least common multiple of  $r_1, \dots, r_w$  is denoted by  $L$ . Then by projecting onto those coordinates corresponding to the  $e_i$  that are equal to one of the  $r_1, \dots, r_w$ , we see again by [5, Theorem 4] that this projection is a  $(0, k_{r_1} + \dots + k_{r_w})$ -sequence in base  $b^L$ . Hence we obtain the necessary condition  $k_{r_1} + \dots + k_{r_w} \leq b^L$ . In particular, if  $\text{lcm}(r_1, \dots, r_w) = r_w$ , then we get  $k_{r_1} + \dots + k_{r_w} \leq b^{r_w}$  as a necessary condition. The latter condition yields a considerable refinement of Theorem 4.

## 4 Mixed ordered orthogonal arrays

We extend our findings regarding the connection between mixed orthogonal arrays and  $(u, m, \mathbf{e}, s)$ -nets further. It is known that classical  $(u, m, s)$ -nets are closely related to the concept of ordered orthogonal arrays, a generalization of orthogonal arrays (see [1, Section 6.2]). We now discuss an analogous relationship between  $(u, m, \mathbf{e}, s)$ -nets and ordered orthogonal arrays over more than one alphabet which we call mixed ordered orthogonal arrays.

Consider a  $(u, m, \mathbf{e}, s)$ -net  $\mathcal{P}$  in base  $b$  with  $b \geq 2$ ,  $s \geq 2$ , and  $\mathbf{e} = (e_1, \dots, e_s) \in \mathbb{N}^s$ , where we again assume without loss of generality that  $e_1 \leq e_2 \leq \dots \leq e_s$ . We suppose that  $m$  is an integer with  $m \geq u + e_s$ .

Choose positive integers  $\beta_i \leq \lfloor (m - u)/e_i \rfloor$  for  $1 \leq i \leq s$ . Let the points of the net  $\mathcal{P}$  be

$$\mathbf{x}_n = (x_n^{(1)}, \dots, x_n^{(s)}) \in [0, 1)^s \quad \text{for } n = 1, \dots, b^m,$$

where

$$x_n^{(i)} = \sum_{l=1}^m x_{l,n}^{(i)} b^{-l} \quad \text{for } 1 \leq n \leq b^m \text{ and } 1 \leq i \leq s,$$

with all  $x_{l,n}^{(i)} \in R(b)$ . For  $1 \leq n \leq b^m$  and  $1 \leq i \leq s$ ,  $1 \leq \rho_i \leq \beta_i$ , define

$$z_{i,\rho_i}(n) := b^{\rho_i e_i} \sum_{l=(\rho_i-1)e_i+1}^{\rho_i e_i} x_{l,n}^{(i)} b^{-l} \in R(b^{e_i}).$$

Arrange these integers into the  $b^m \times (\beta_1 + \dots + \beta_s)$  array

$$\begin{aligned} Z &= (z_{i,\rho_i}(n))_{1 \leq n \leq b^m; 1 \leq i \leq s, 1 \leq \rho_i \leq \beta_i} = \\ &= \begin{pmatrix} z_{1,1}(1) & \dots & z_{1,\beta_1}(1) & \dots & \dots & z_{s,1}(1) & \dots & z_{s,\beta_s}(1) \\ z_{1,1}(2) & \dots & z_{1,\beta_1}(2) & \dots & \dots & z_{s,1}(2) & \dots & z_{s,\beta_s}(2) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ z_{1,1}(b^m) & \dots & z_{1,\beta_1}(b^m) & \dots & \dots & z_{s,1}(b^m) & \dots & z_{s,\beta_s}(b^m) \end{pmatrix}. \end{aligned}$$

Now we show the following property of this array, with an obvious notation for the columns of  $Z$  (compare with the proof of Theorem 1).

**Proposition 2.** *Let  $\mathcal{P}$  be a  $(u, m, \mathbf{e}, s)$ -net in base  $b$  and let  $Z$  be the array obtained from  $\mathcal{P}$  as described above. Choose an integer  $t$  with  $1 \leq t \leq s$  and integers  $1 \leq i_1 < i_2 < \dots <$*

$i_t \leq s$ . Furthermore, choose positive integers  $\kappa_{i_1}, \dots, \kappa_{i_t}$  such that  $\kappa_{i_j} \leq \beta_{i_j}$  for  $1 \leq j \leq t$  and

$$\sum_{j=1}^t \kappa_{i_j} e_{i_j} \leq m - u.$$

Then the columns

$$\mathbf{z}_{i_1,1}, \dots, \mathbf{z}_{i_1,\kappa_{i_1}}, \mathbf{z}_{i_2,1}, \dots, \mathbf{z}_{i_2,\kappa_{i_2}}, \dots, \mathbf{z}_{i_t,1}, \dots, \mathbf{z}_{i_t,\kappa_{i_t}}$$

of the array  $Z$  are orthogonal in the sense that, with  $d = \sum_{j=1}^t \kappa_{i_j}$ , every possible  $d$ -tuple occurs an equal number of times as a row in the  $b^m \times d$  subarray of  $Z$  formed by these columns.

*Proof.* Take any  $(h_1^{(j)}, \dots, h_{\kappa_{i_j}}^{(j)}) \in (R(b^{e_{i_j}}))^{\kappa_{i_j}}$  for  $1 \leq j \leq t$ . For  $1 \leq n \leq b^m$  we have

$$(z_{i_1,1}(n), \dots, z_{i_1,\kappa_{i_1}}(n), \dots, z_{i_t,1}(n), \dots, z_{i_t,\kappa_{i_t}}(n)) = (h_1^{(1)}, \dots, h_{\kappa_{i_1}}^{(1)}, \dots, h_1^{(t)}, \dots, h_{\kappa_{i_t}}^{(t)}) \quad (6)$$

if and only if  $z_{i_j,\rho_{i_j}}(n) = h_{\rho_{i_j}}^{(j)}$  for  $1 \leq j \leq t$  and  $1 \leq \rho_{i_j} \leq \kappa_{i_j}$ . The latter condition means that

$$b^{\rho_{i_j} e_{i_j}} \sum_{l=(\rho_{i_j}-1)e_{i_j}+1}^{\rho_{i_j} e_{i_j}} x_{l,n}^{(i_j)} b^{-l} = h_{\rho_{i_j}}^{(j)}$$

for  $1 \leq j \leq t$  and  $1 \leq \rho_{i_j} \leq \kappa_{i_j}$ , which is equivalent to

$$\sum_{l=(\rho_{i_j}-1)e_{i_j}+1}^{\rho_{i_j} e_{i_j}} \frac{x_{l,n}^{(i_j)}}{b^l} = \frac{h_{\rho_{i_j}}^{(j)}}{b^{\rho_{i_j} e_{i_j}}}$$

for  $1 \leq j \leq t$  and  $1 \leq \rho_{i_j} \leq \kappa_{i_j}$ . This is, in turn, equivalent to

$$x_n^{(i_j)} \in \left[ \sum_{\rho_{i_j}=1}^{\kappa_{i_j}} \frac{h_{\rho_{i_j}}^{(j)}}{b^{\rho_{i_j} e_{i_j}}}, \sum_{\rho_{i_j}=1}^{\kappa_{i_j}} \frac{h_{\rho_{i_j}}^{(j)}}{b^{\rho_{i_j} e_{i_j}}} + \frac{1}{b^{\kappa_{i_j} e_{i_j}}} \right) =: \left[ \frac{a^{(i_j)}}{b^{\kappa_{i_j} e_{i_j}}}, \frac{a^{(i_j)} + 1}{b^{\kappa_{i_j} e_{i_j}}} \right),$$

for  $1 \leq j \leq t$ , for some integers  $a^{(i_j)} \in \{0, 1, \dots, b^{\kappa_{i_j} e_{i_j}} - 1\}$ . Thus, (6) is equivalent to

$$\mathbf{x}_n \in J := \prod_{i=1}^s J_i,$$

where

$$J_i = \begin{cases} [0, 1) & \text{if } i \notin \{i_1, \dots, i_t\}, \\ [a^{(i_j)}/b^{\kappa_{i_j} e_{i_j}}, (a^{(i_j)} + 1)/b^{\kappa_{i_j} e_{i_j}}) & \text{if } i = i_j \text{ for some } 1 \leq j \leq t. \end{cases}$$

However, the interval  $J$  is an elementary interval in base  $b$  of volume

$$b^{-\kappa_{i_1} e_{i_1} - \dots - \kappa_{i_t} e_{i_t}} \geq b^{u-m}.$$

Hence the definition of a  $(u, m, \mathbf{e}, s)$ -net in base  $b$  applies. Therefore the number of integers  $n$  with  $1 \leq n \leq b^m$  such that (6) holds is given by

$$b^m b^{-\kappa_{i_1} e_{i_1} - \dots - \kappa_{i_t} e_{i_t}}$$

for all  $(h_1^{(1)}, \dots, h_{\kappa_{i_1}}^{(1)}, \dots, h_1^{(t)}, \dots, h_{\kappa_{i_t}}^{(t)})$ , and the desired orthogonality property is established.  $\square$



We call the array

$$Z = (z_{i,\rho_i}(n))_{1 \leq n \leq b^m; 1 \leq i \leq s, 1 \leq \rho_i \leq \beta_i}$$

obtained from a  $(u, m, \mathbf{e}, s)$ -net  $\mathcal{P}$  in base  $b$  a *mixed ordered orthogonal array* and denote it by

$$\text{OOA}(b^m, (\beta_1, \dots, \beta_s), l_1^1 \cdots l_s^1, m - u), \quad (7)$$

where  $l_i = b^{e_i}$  for  $1 \leq i \leq s$ . We call  $m - u$  the *strength* of  $Z$ . The reason why we choose the notation (7) for  $Z$  is as follows. If all  $e_i = 1$ , i.e., if  $l_i = b$  for  $1 \leq i \leq s$ , then a  $(u, m, \mathbf{e}, s)$ -net in base  $b$  simplifies to a  $(u, m, s)$ -net in base  $b$ . In this case, we may choose all  $\beta_i$  equal to  $m - u$ , and then we obtain a classical ordered orthogonal array with  $b^m$  rows,  $s(m - u)$  columns, and strength  $m - u$  from the net. The connection between  $(u, m, s)$ -nets and classical ordered orthogonal arrays is well known (see [1, Section 6.2] and [10]).

So far, we have shown that a  $(u, m, \mathbf{e}, s)$ -net in base  $b$  yields a mixed ordered orthogonal array

$$\text{OOA}(b^m, (\beta_1, \dots, \beta_s), l_1^1 \cdots l_s^1, m - u)$$

with  $1 \leq \beta_i \leq \lfloor (m - u)/e_i \rfloor$  and  $l_i = b^{e_i}$  for  $1 \leq i \leq s$ . We are now going to prove that the converse is also true.

Let  $e_1, \dots, e_s \in \mathbb{N}$ . Choose  $\beta_i = \lfloor (m - u)/e_i \rfloor$  for  $1 \leq i \leq s$ , where  $m$  and  $u$  are integers with  $m \geq u + e_s$  and  $u \geq 0$ . Suppose now that  $Z$  is a  $b^m \times (\beta_1 + \dots + \beta_s)$  array with entries  $z_{i,\rho_i}(n) \in R(b^{e_i})$  for  $1 \leq n \leq b^m$ ,  $1 \leq i \leq s$ ,  $1 \leq \rho_i \leq \beta_i$ . Suppose furthermore that  $Z$  satisfies the following condition: for every choice of  $t \in \{1, \dots, s\}$  and  $\kappa_{i_1}, \dots, \kappa_{i_t} \in \mathbb{N}$  such that  $\kappa_{i_j} \leq \beta_{i_j}$  for  $1 \leq j \leq t$  and

$$\sum_{j=1}^t \kappa_{i_j} e_{i_j} \leq m - u,$$

the columns

$$\mathbf{z}_{i_1,1}, \dots, \mathbf{z}_{i_1,\kappa_{i_1}}, \dots, \mathbf{z}_{i_t,1}, \dots, \mathbf{z}_{i_t,\kappa_{i_t}}$$

of  $Z$  have the property that each

$$(h_1^{(1)}, \dots, h_{\kappa_{i_1}}^{(1)}, \dots, h_1^{(t)}, \dots, h_{\kappa_{i_t}}^{(t)}) \in (R(b^{e_{i_1}}))^{\kappa_{i_1}} \times \dots \times (R(b^{e_{i_t}}))^{\kappa_{i_t}}$$

occurs with frequency

$$b^m b^{-\kappa_{i_1} e_{i_1} - \dots - \kappa_{i_t} e_{i_t}}.$$

As we will show,  $Z$  yields a  $(u, m, \mathbf{e}, s)$ -net in base  $b$ . Indeed, let  $z_{i,\rho_i}(n) \in R(b^{e_i})$ , where  $1 \leq n \leq b^m$ ,  $1 \leq i \leq s$ ,  $1 \leq \rho_i \leq \beta_i$ , be an entry of  $Z$ . Then  $z_{i,\rho_i}(n)$  has an expansion in base  $b$  of the form

$$z_{i,\rho_i}(n) = \sum_{l=0}^{e_i-1} x_{\rho_i e_i - l, n}^{(i)} b^l = b^{\rho_i e_i} \sum_{l=(\rho_i-1)e_i+1}^{\rho_i e_i} x_{l,n}^{(i)} b^{-l},$$

where  $x_{(\rho_i-1)e_i+1,n}^{(i)}, \dots, x_{\rho_i e_i,n}^{(i)} \in R(b)$ .

Hence from the entries  $z_{i,1}(n), \dots, z_{i,\beta_i}(n)$  we obtain digits  $x_{1,n}^{(i)}, \dots, x_{\beta_i e_i,n}^{(i)} \in R(b)$  for all  $1 \leq i \leq s$  and  $1 \leq n \leq b^m$ . We use these digits to define

$$x_n^{(i)} := \sum_{l=1}^{\beta_i e_i} x_{l,n}^{(i)} b^{-l} \in [0, 1)$$

for  $1 \leq i \leq s$  and  $1 \leq n \leq b^m$ . Finally, we put

$$\mathbf{x}_n := (x_n^{(1)}, \dots, x_n^{(s)}) \in [0, 1]^s \quad \text{for } 1 \leq n \leq b^m.$$

We claim that  $\mathbf{x}_1, \dots, \mathbf{x}_{b^m}$  form a  $(u, m, \mathbf{e}, s)$ -net in base  $b$ . We denote the point set consisting of the  $\mathbf{x}_n$  by  $\mathcal{P}$ .

In order to verify the desired net property of  $\mathcal{P}$ , let  $J = \prod_{i=1}^s J_i$  be an elementary interval in base  $b$  for which there exist a  $t \in \{1, \dots, s\}$  and indices  $i_1, \dots, i_t \in \{1, \dots, s\}$ ,  $1 \leq i_1 < i_2 < \dots < i_t \leq s$ , such that

$$J_i = \begin{cases} [0, 1) & \text{if } i \notin \{i_1, \dots, i_t\}, \\ [a^{(i_j)}/b^{\kappa_{i_j}e_{i_j}}, (a^{(i_j)} + 1)/b^{\kappa_{i_j}e_{i_j}}) & \text{if } i = i_j \text{ for some } 1 \leq j \leq t, \end{cases}$$

where the  $a^{(i_j)}$  are integers satisfying  $0 \leq a^{(i_j)} < b^{\kappa_{i_j}e_{i_j}}$  for all  $1 \leq j \leq t$  and where the  $\kappa_{i_1}, \dots, \kappa_{i_t}$  are positive integers with

$$\sum_{j=1}^t \kappa_{i_j} e_{i_j} \leq m - u,$$

that is,  $\lambda_s(J) \geq b^{u-m}$ . Note that the condition on the  $\kappa_{i_j}$  implies that no  $\kappa_{i_j}$  exceeds  $\beta_{i_j}$ . We need to show that  $J$  contains exactly

$$b^m b^{-\kappa_{i_1}e_{i_1} - \dots - \kappa_{i_t}e_{i_t}}$$

points of  $\mathcal{P}$ . Suppose that  $n$  is such that  $\mathbf{x}_n \in J$ , i.e.,

$$x_n^{(i_j)} \in \left[ \frac{a^{(i_j)}}{b^{\kappa_{i_j}e_{i_j}}}, \frac{a^{(i_j)} + 1}{b^{\kappa_{i_j}e_{i_j}}} \right)$$

for  $1 \leq j \leq t$ . Since  $0 \leq a^{(i_j)} < b^{\kappa_{i_j}e_{i_j}}$ , we can represent  $a^{(i_j)}/b^{\kappa_{i_j}e_{i_j}}$  as

$$\frac{a^{(i_j)}}{b^{\kappa_{i_j}e_{i_j}}} = \sum_{\rho_{i_j}=1}^{\kappa_{i_j}} \frac{h_{\rho_{i_j}}^{(j)}}{b^{\rho_{i_j}e_{i_j}}}$$

for some  $h_1^{(j)}, \dots, h_{\kappa_{i_j}}^{(j)} \in R(b^{e_{i_j}})$ . Then  $\mathbf{x}_n \in J$  is equivalent to

$$x_n^{(i_j)} \in \left[ \sum_{\rho_{i_j}=1}^{\kappa_{i_j}} \frac{h_{\rho_{i_j}}^{(j)}}{b^{\rho_{i_j}e_{i_j}}}, \sum_{\rho_{i_j}=1}^{\kappa_{i_j}} \frac{h_{\rho_{i_j}}^{(j)}}{b^{\rho_{i_j}e_{i_j}}} + \frac{1}{b^{\kappa_{i_j}e_{i_j}}} \right)$$

for all  $j \in \{1, \dots, t\}$ . This, however, is equivalent to

$$\sum_{l=(\rho_{i_j}-1)e_{i_j}+1}^{\rho_{i_j}e_{i_j}} \frac{x_{l,n}^{(i_j)}}{b^l} = \frac{h_{\rho_{i_j}}^{(j)}}{b^{\rho_{i_j}e_{i_j}}}$$

for  $1 \leq j \leq t$  and  $1 \leq \rho_{i_j} \leq \kappa_{i_j}$ , which means that

$$z_{i_j, \rho_{i_j}}(n) = b^{\rho_{i_j}e_{i_j}} \sum_{l=(\rho_{i_j}-1)e_{i_j}+1}^{\rho_{i_j}e_{i_j}} x_{l,n}^{(i_j)} b^{-l} = h_{\rho_{i_j}}^{(j)}$$

for  $1 \leq j \leq t$  and  $1 \leq \rho_{i_j} \leq \kappa_{i_j}$ . By the orthogonality properties of the columns of  $Z$  that we assumed above, the latter condition is fulfilled for exactly

$$b^m b^{-\kappa_{i_1} e_{i_1} - \dots - \kappa_{i_t} e_{i_t}}$$

indices  $n$ . This shows that  $\mathcal{P}$  is indeed a  $(u, m, \mathbf{e}, s)$ -net in base  $b$ . In summary, we have shown the following result.

**Theorem 5.** *The existence of a  $(u, m, \mathbf{e}, s)$ -net in base  $b$  is equivalent to the existence of a mixed ordered orthogonal array*

$$\text{OOA}(b^m, (\beta_1, \dots, \beta_s), l_1^1 \dots l_s^1, m - u)$$

with  $l_i = b^{e_i}$  and  $\beta_i = \lfloor (m - u)/e_i \rfloor$  for  $1 \leq i \leq s$ .

**Remark 5.** Theorem 5 can be used for the construction of mixed ordered orthogonal arrays, by starting from a known construction of a  $(u, m, \mathbf{e}, s)$ -net. A powerful construction of such nets was presented in [5, Section 5] and it employs global function fields, that is, algebraic function fields of one variable over a finite field. We use the standard terminology for global function fields in the monographs [16] and [19]. Let  $F$  be a global function field with full constant field  $\mathbb{F}_q$ , where  $q$  is an arbitrary prime power, and let  $g(F)$  be the genus of  $F$ . For an integer  $s \geq 2$ , let  $P_1, \dots, P_s$  be  $s$  distinct places of  $F$ . Let  $e_i$  be the degree of  $P_i$  for  $1 \leq i \leq s$  and put  $\mathbf{e} = (e_1, \dots, e_s) \in \mathbb{N}^s$ . Then for every integer  $m \geq \max(1, g(F))$  which is a multiple of  $\text{lcm}(e_1, \dots, e_s)$ , there is a construction of a  $(u, m, \mathbf{e}, s)$ -net in base  $q$  with  $u = g(F)$ . The condition on  $m$  can be relaxed in many cases (see [5, Remark 3]). Mixed ordered orthogonal arrays corresponding to these nets can be read off from Theorem 5.

## 5 A bound for mixed ordered orthogonal arrays

Throughout this section, let  $Z$  be a mixed ordered orthogonal array (7) obtained from a  $(u, m, \mathbf{e}, s)$ -net in base  $b$  according to Proposition 2. We denote by  $C$  the collection of all columns of  $Z$  and, for  $1 \leq i \leq s$ , we define  $C_i$  to be the collection of the columns  $\mathbf{z}_{i,1}, \dots, \mathbf{z}_{i,\beta_i}$  of  $Z$ . We generalize the argumentation in [10], which corresponds to the special case  $e_i = 1$  for  $1 \leq i \leq s$ .

Suppose that  $D := (D_1, \dots, D_s)$  is an  $s$ -tuple of functions, where

$$D_i : C_i \rightarrow R(b^{e_i}) \quad \text{for } 1 \leq i \leq s.$$

For two functions  $D_i^{(1)}, D_i^{(2)}$ , both mapping from  $C_i$  to  $R(b^{e_i})$ , we define  $D_i^{(1)} - D_i^{(2)}$  by

$$(D_i^{(1)} - D_i^{(2)})(\mathbf{z}) := D_i^{(1)}(\mathbf{z}) - D_i^{(2)}(\mathbf{z}) \pmod{b^{e_i}}.$$

We now define two quantities that are associated with an  $s$ -tuple  $D = (D_1, \dots, D_s)$  as given above. First, we define the profile of  $D = (D_1, \dots, D_s)$  by

$$\text{PROFILE}(D) = \text{PROFILE}((D_1, \dots, D_s)) := (d_1, \dots, d_s),$$

where

$$d_i = \begin{cases} 0 & \text{if } D_i(\mathbf{z}_{i,\rho_i}) = 0 \text{ for } 1 \leq \rho_i \leq \beta_i, \\ \max\{\rho_i : D_i(\mathbf{z}_{i,\rho_i}) \neq 0\} & \text{otherwise,} \end{cases}$$

for  $1 \leq i \leq s$ . Note that  $0 \leq d_i \leq \beta_i$  for  $1 \leq i \leq s$ . Furthermore, we define the height of  $D = (D_1, \dots, D_s)$  as

$$\text{HEIGHT}(D) = \text{HEIGHT}((D_1, \dots, D_s)) := \sum_{i=1}^s d_i e_i.$$

Moreover, note that if  $Z$  is a mixed ordered orthogonal array (7) obtained from a  $(u, m, \mathbf{e}, s)$ -net in base  $b$  according to Proposition 2 and if

$$\text{HEIGHT}((D_1, \dots, D_s)) = \sum_{i=1}^s d_i e_i \leq m - u,$$

then the columns

$$\mathbf{z}_{1,1}, \dots, \mathbf{z}_{1,\delta_1}, \dots, \mathbf{z}_{s,1}, \dots, \mathbf{z}_{s,\delta_s}$$

are orthogonal for all  $\delta_j \leq d_j$ ,  $1 \leq j \leq s$ , by Proposition 2.

We now show the following theorem which is the “mixed” analog of [10, Lemma 3.1]. This theorem gives a necessary condition on the parameters of a mixed ordered orthogonal array.

**Theorem 6.** *Let  $Z$  be a mixed ordered orthogonal array (7) obtained from a  $(u, m, \mathbf{e}, s)$ -net in base  $b$ . Let  $\mathcal{D}$  be a set of functions defined on  $C$  such that*

$$\text{HEIGHT}((D_1^{(1)}, \dots, D_s^{(1)}) - (D_1^{(2)}, \dots, D_s^{(2)})) \leq m - u$$

for all  $(D_1^{(1)}, \dots, D_s^{(1)}), (D_1^{(2)}, \dots, D_s^{(2)}) \in \mathcal{D}$ . Then  $b^m \geq |\mathcal{D}|$ .

*Proof.* Let  $\omega_j := e^{2\pi i/b^{e_j}} \in \mathbb{C}$  and let  $1, \omega_j, \omega_j^2, \dots, \omega_j^{b^{e_j}-1}$  be the  $b^{e_j}$ -th roots of unity for  $1 \leq j \leq s$ . Suppose now that  $Z$  is as in the theorem. Let  $C$  and  $C_i$ ,  $1 \leq i \leq s$ , be as in the beginning of this section. We can identify a column  $\mathbf{c} \in C_i$  with a vector  $v_{\mathbf{c}}$  over the alphabet  $1, \omega_i, \dots, \omega_i^{b^{e_i}-1}$ , that is,  $v_{\mathbf{c}} \in \mathbb{C}^{b^m}$ .

Let  $D = (D_1, \dots, D_s) \in \mathcal{D}$ , where  $D_i : C_i \rightarrow R(b^{e_i})$  for  $1 \leq i \leq s$ . For every  $\mathbf{c} \in C$ , we can identify a unique  $i \in \{1, \dots, s\}$  such that  $\mathbf{c} \in C_i$ , and we take  $D_i(\mathbf{c})$  copies of the corresponding  $v_{\mathbf{c}} \in \mathbb{C}^{b^m}$ . We repeat this procedure for each  $\mathbf{c} \in C$  and we obtain

$$\sum_{i=1}^s \sum_{\rho_i=1}^{\beta_i} D_i(\mathbf{z}_{i,\rho_i})$$

vectors in  $\mathbb{C}^{b^m}$ . We then take the componentwise product of these vectors and thereby obtain a vector  $v_D \in \mathbb{C}^{b^m}$  determined by  $D$ . This vector is of the form

$$\begin{pmatrix} \prod_{i=1}^s \prod_{\rho_i=1}^{\beta_i} \omega_i^{k_{i,\rho_i}^{(1)} D_i(\mathbf{z}_{i,\rho_i})} \\ \vdots \\ \prod_{i=1}^s \prod_{\rho_i=1}^{\beta_i} \omega_i^{k_{i,\rho_i}^{(b^m)} D_i(\mathbf{z}_{i,\rho_i})} \end{pmatrix}$$

with the  $k_{i,\rho_i}^{(n)}$  being elements of  $R(b^{e_i})$  for  $1 \leq i \leq s$  and  $1 \leq \rho_i \leq \beta_i$ . For two distinct elements  $D^{(1)} = (D_1^{(1)}, \dots, D_s^{(1)})$  and  $D^{(2)} = (D_1^{(2)}, \dots, D_s^{(2)})$  of  $\mathcal{D}$ , we have by assumption,

$$\text{HEIGHT}(D^{(1)} - D^{(2)}) \leq m - u.$$

For short, we write  $E := D^{(1)} - D^{(2)}$ , with  $E_i = D_i^{(1)} - D_i^{(2)}$  for  $1 \leq i \leq s$ . Hence we know that  $\text{HEIGHT}(E) \leq m - u$ . Thus, there exist integers  $d_1, \dots, d_s$  with  $0 \leq d_i \leq \beta_i$  for  $1 \leq i \leq s$  such that  $\sum_{i=1}^s d_i e_i \leq m - u$  and  $E_i(\mathbf{z}_{i,\rho_i}) = 0$  for  $\rho_i > d_i$ . Formulating this property of  $E$  slightly differently, we can say that there exist positive integers  $\kappa_{i_1}, \dots, \kappa_{i_t}$  with  $1 \leq i_1 < \dots < i_t \leq s$  and  $\kappa_{i_j} \leq \beta_{i_j}$  for  $1 \leq j \leq t$  such that

$$\sum_{j=1}^t \kappa_{i_j} e_{i_j} \leq m - u$$

as well as  $E_i(\mathbf{z}_{i,\rho_i}) > 0$  if and only if  $i = i_j$  for some  $j$  and  $\rho_{i_j} \leq \kappa_{i_j}$ . By Proposition 2, the columns

$$\mathbf{z}_{i_1,1}, \dots, \mathbf{z}_{i_1,\kappa_{i_1}}, \dots, \mathbf{z}_{i_t,1}, \dots, \mathbf{z}_{i_t,\kappa_{i_t}}$$

are orthogonal, and so also the  $v_{\mathbf{c}}$  corresponding to these columns of  $Z$  are orthogonal and each possible combination of symbols occurs with frequency  $f = b^m b^{-\kappa_{i_1} e_{i_1} - \dots - \kappa_{i_t} e_{i_t}}$ . Let now  $\langle \cdot, \cdot \rangle$  denote the usual Hermitian inner product in  $\mathbb{C}^{b^m}$ . We study the expression

$$\begin{aligned} \langle v_{D^{(1)}}, v_{D^{(2)}} \rangle &= \sum_{n=1}^{b^m} \prod_{i=1}^s \prod_{\rho_i=1}^{\beta_i} \omega_i^{k_{i,\rho_i}^{(n)} E_i(\mathbf{z}_{i,\rho_i})} \\ &= \sum_{n=1}^{b^m} \prod_{j=1}^t \prod_{\rho_{i_j}=1}^{\kappa_{i_j}} \omega_{i_j}^{k_{i_j,\rho_{i_j}}^{(n)} E_{i_j}(\mathbf{z}_{i_j,\rho_{i_j}})}. \end{aligned}$$

Due to the above-mentioned orthogonality properties of the  $v_{\mathbf{c}}$ , we can write

$$\begin{aligned} \langle v_{D^{(1)}}, v_{D^{(2)}} \rangle &= f \sum_{k_{i_1,1}=0}^{b^{e_{i_1}}-1} \dots \sum_{k_{i_1,\kappa_{i_1}}=0}^{b^{e_{i_1}}-1} \dots \sum_{k_{i_t,1}=0}^{b^{e_{i_t}}-1} \dots \sum_{k_{i_t,\kappa_{i_t}}=0}^{b^{e_{i_t}}-1} \prod_{j=1}^t \prod_{\rho_{i_j}=1}^{\kappa_{i_j}} \omega_{i_j}^{k_{i_j,\rho_{i_j}} E_{i_j}(\mathbf{z}_{i_j,\rho_{i_j}})} \\ &= f \prod_{j=1}^t \prod_{\rho_{i_j}=1}^{\kappa_{i_j}} \sum_{k_{i_j,\rho_{i_j}}=0}^{b^{e_{i_j}}-1} \omega_{i_j}^{k_{i_j,\rho_{i_j}} E_{i_j}(\mathbf{z}_{i_j,\rho_{i_j}})}. \end{aligned}$$

However, as  $E_{i_j}(\mathbf{z}_{i_j,\rho_{i_j}}) \not\equiv 0 \pmod{b^{e_{i_j}}}$  in the last sum, it is clear that

$$\sum_{k_{i_j,\rho_{i_j}}=0}^{b^{e_{i_j}}-1} \omega_{i_j}^{k_{i_j,\rho_{i_j}} E_{i_j}(\mathbf{z}_{i_j,\rho_{i_j}})} = \sum_{k_{i_j,\rho_{i_j}}=0}^{b^{e_{i_j}}-1} \left( \omega_{i_j}^{E_{i_j}(\mathbf{z}_{i_j,\rho_{i_j}})} \right)^{k_{i_j,\rho_{i_j}}} = 0.$$

We therefore see that the collection of the  $v_D$  with  $D \in \mathcal{D}$  is orthogonal with respect to  $\langle \cdot, \cdot \rangle$ , and therefore  $\{v_D : D \in \mathcal{D}\}$  is a linearly independent set of vectors in  $\mathbb{C}^{b^m}$ . This implies the desired result.  $\square$

**Remark 6.** A natural question is whether one can derive effective concrete bounds on the  $u$ -value of  $(u, m, \mathbf{e}, s)$ -nets in base  $b$  from Theorem 6, as it was done analogously for ordinary  $(u, m, s)$ -nets in [10]. However, this question appears to be very challenging, and is therefore left open for future research.

## References

- [1] J. Dick, F. Pillichshammer. *Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration*. Cambridge University Press, Cambridge, 2010.
- [2] A.S. Hedayat, N.J.A. Sloane, J. Stufken. *Orthogonal Arrays: Theory and Applications*. Springer, New York, 1999.
- [3] R. Hofer. Generalized Hofer-Niederreiter sequences and their discrepancy from a  $(\mathbf{U}, \mathbf{e}, s)$ -point of view. *J. Complexity* 31, 260–276, 2015.
- [4] R. Hofer, H. Niederreiter. A construction of  $(t, s)$ -sequences with finite-row generating matrices using global function fields. *Finite Fields Appl.* 21, 97–110, 2013.
- [5] P. Kritzer, H. Niederreiter. Propagation rules for  $(u, m, \mathbf{e}, s)$ -nets and  $(u, \mathbf{e}, s)$ -sequences. *J. Complexity* 31, 457–473, 2015.
- [6] K.M. Lawrence. A combinatorial characterization of  $(t, m, s)$ -nets in base  $b$ . *J. Combinatorial Designs* 4, 275–293, 1996.
- [7] C.F. Laywine, G.L. Mullen. *Discrete Mathematics Using Latin Squares*. Wiley, New York, 1998.
- [8] G. Leobacher, F. Pillichshammer. *Introduction to Quasi-Monte Carlo Integration and Applications*. Birkhäuser and Springer International, Heidelberg, 2014.
- [9] R. Lidl, H. Niederreiter. *Introduction to Finite Fields and Their Applications*, revised edition. Cambridge University Press, Cambridge, 1994.
- [10] W.J. Martin, D.R. Stinson. A generalized Rao bound for ordered orthogonal arrays and  $(t, m, s)$ -nets. *Canad. Math. Bull.* 42, 359–370, 1999.
- [11] G.L. Mullen, W.Ch. Schmid. An equivalence between  $(t, m, s)$ -nets and strongly orthogonal hypercubes. *J. Combinatorial Theory Ser. A* 76, 164–174, 1996.
- [12] H. Niederreiter. Point sets and sequences with small discrepancy. *Monatsh. Math.* 104, 273–337, 1987.
- [13] H. Niederreiter. *Random Number Generation and Quasi-Monte Carlo Methods*. SIAM, Philadelphia, 1992.
- [14] H. Niederreiter.  $(t, m, s)$ -nets and  $(t, s)$ -sequences. *Handbook of Finite Fields* (G.L. Mullen, D. Panario, eds.), pp. 619–630, CRC Press, Boca Raton, FL, 2013.
- [15] H. Niederreiter, C.P. Xing. *Rational Points on Curves over Finite Fields: Theory and Applications*. Cambridge University Press, Cambridge, 2001.
- [16] H. Niederreiter, C.P. Xing. *Algebraic Geometry in Coding Theory and Cryptography*. Princeton University Press, Princeton, NJ, 2009.
- [17] H. Niederreiter, A.S.J. Yeo. Halton-type sequences from global function fields. *Science China Math.* 56, 1467–1476, 2013.

- [18] R. Schürer, W.Ch. Schmid. MinT – new features and new results. *Monte Carlo and Quasi-Monte Carlo Methods 2008* (P. L’Ecuyer, A.B. Owen, eds.), pp. 171–189, Springer, Berlin, 2009.
- [19] H. Stichtenoth. *Algebraic Function Fields and Codes*, second edition. Springer, Berlin, 2009.
- [20] S. Tezuka. On the discrepancy of generalized Niederreiter sequences. *J. Complexity* 29, 240–247, 2013.

**Authors’ addresses:**

Peter Kritzer

Department of Financial Mathematics and Applied Number Theory,  
Johannes Kepler University Linz,  
Altenbergerstr. 69, A-4040 Linz, AUSTRIA.  
`peter.kritzer@jku.at`

Harald Niederreiter

Johann Radon Institute for Computational and Applied Mathematics,  
Austrian Academy of Sciences,  
Altenbergerstr. 69, A-4040 Linz, AUSTRIA,  
and  
Department of Mathematics,  
University of Salzburg,  
Hellbrunnerstr. 34, A-5020 Salzburg, AUSTRIA,  
`ghnied@gmail.com`